N

Office of the Attorney General
Washington, D. C. 20530

March 31, 1982

MEMORANDUM FOR THE PRESIDENT

SUBJECT: Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information

At the request of William P. Clark, I convened an interdepartmental group to study the effectiveness of existing statutes and Executive orders prohibiting unauthorized disclosure of classified information. This group was chaired by Deputy Assistant Attorney General Richard K. Willard and included representatives of the Secretaries of State, the Treasury, Defense, and Energy, and the Director of Central Intelligence. Attached is the report of this group.

Unauthorized disclosure of classified information constitutes a serious threat to our national security. It is a complex problem that cannot be solved easily or quickly. However, the effectiveness of our enforcement effort can be improved by adopting the recommendations of this report, which I endorse.

William French Smith
Attorney General

Attachment

DOJ Review Completed.

cc: The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Secretary of Energy
The Director of Central Intelligence
The Assistant to the President for National Security Affairs

REPORT OF THE INTERDEPARTMENTAL GROUP ON UNAUTHORIZED DISCLOSURES OF CLASSIFIED INFORMATION

March 31, 1982

Chairman:

Richard K. Willard
Deputy Assistant Attorney General
Department of Justice

Members:

Daniel W. McGovern
Deputy Legal Adviser
Department of State

Jordan Luke
Assistant General Counsel
Department of the Treasury

Kathleen A. Buck
Assistant General Counsel

L. Britt Snider
Director for Counterintelligence
and Security Policy
Department of Defense

James W. Culpepper
Deputy Assistant Secretary
for Security Affairs
Department of Energy

[redacted] STAT
Deputy General Counsel
Central Intelligence Agency

Introduction

This interdepartmental group was convened by Attorney General William French Smith at the request of William P. Clark, the Assistant to the President for National Security Affairs. Members of the group were designated by the heads of participating departments and agencies. The group met throughout February and March of 1982, and this report generally reflects the consensus of the individual participants. However, the report and its recommendations have not received the approval of the participating departments and agencies. We anticipate that the proposed National Security Decision Directive would be circulated for formal agency comment before being approved.

RICHARD K. WILLARD
Deputy Assistant Attorney General
Department of Justice
Chairman

Table of Contents

A. Executive Summary

B. Nature of the Problem and Scope of Report

C. Laws Pertaining to Unauthorized Disclosures

D. Protective Security Programs

E. Past Experience with Leak Investigations

F. Proposed New Approach to Leak Investigations

G. Draft National Security Decision Directive

Approved For Release 2007/08/06 : CIA-RDP84B00049R001002600037-8

Tab A

EXECUTIVE SUMMARY

Unauthorized disclosure of classified information is a long-standing problem that has increased in severity over the past decade. This problem has resisted efforts at solution under a number of Administrations. Yet the protection of national security information remains a fundamental constitutional duty of the President. The continuing large number of unauthorized disclosures has damaged the national security interests of the United States and has raised serious questions about the government's ability to protect its most sensitive secrets from disclosure in the media. We must seek more effective means to prevent, deter, and punish unauthorized disclosures. At the same time, we must recognize that this complex problem is unlikely to be solved easily or quickly.

The scope of this report is limited to unauthorized disclosures of classified information where there is no apparent involvement of a foreign power. Such disclosures primarily occur through media "leaks" by anonymous government employees, or in publications and statements by former employees. Beyond the scope of this report are the following kinds of disclosures:

--clandestine disclosures of classified information to foreign powers or their agents, which is espionage in the classic sense;

--authorized disclosures of classified information by government officials who are not publicly identified;

--leaks of unclassified information; and

--compromise of classified information through negligence.

Although the foregoing kinds of disclosures also present serious problems, we have limited the scope of this report in order to produce a more comprehensible set of recommendations.

It should be noted that some high ranking officials erroneously believe they have the authority to leak classified information in furtherance of government policy. Such disclosures may only be made by persons with declassification authority under Executive Order 12065 or otherwise from the President. Without

such authority, "friendly" leaks are just as unlawful as any other unauthorized disclosure of classified information.

Laws Pertaining to Unauthorized Disclosures

The unauthorized disclosure of classified information has been specifically prohibited by a series of Executive orders dating back at least to 1951. Such disclosures also violate numerous more general standards of conduct for government employees based on statutes and regulations. It is clear that any government employee may be discharged or otherwise disciplined for making unauthorized disclosures of classified information. Moreover, in virtually all cases the unauthorized disclosure of classified information potentially violates one or more federal criminal statutes.

However, there is no single statute that makes it a crime as such for a government employee to disclose classified information without authorization. With the exception of certain specialized categories of information, the government must ordinarily seek to prosecute unauthorized disclosures as violations of the Espionage Act or as the theft of government property. Such prosecutions have not been undertaken because of a variety of legal and practical problems.

Therefore, it would be helpful if Congress enacted a law providing criminal penalties for government employees who, without authorization, disclose information that is properly classified pursuant to statute or Executive order. Such a law would be appropriate in view of the substantial body of criminal statutes punishing unauthorized disclosure of other kinds of sensitive information by government employees, such as banking, agricultural and census data. Classified national security information deserves at least the same degree of protection.

A promising development in recent years has been the judicial recognition that the government may enforce secrecy agreements through civil litigation. Many government employees sign secrecy agreements as a condition of employment with intelligence agencies or to obtain access to classified information. In a series of cases culminating in the Supreme Court's 1980 decision in United States v. Snepp, the Justice Department has obtained injunctions and monetary remedies from individuals who seek to publish classified information in violation of their secrecy obligations. Such civil litigation avoids many of the procedural problems that would be encountered in criminal prosecutions. The effectiveness of this program would be increased by greater use of properly drafted secrecy agreements.

Protective Security Programs

The overall effectiveness of the government's programs for safeguarding classified information undoubtedly affects the frequency of leaks. Tight security measures--including limiting access to classified information to those with a real "need to know"--reduce the opportunities for unauthorized disclosure. By contrast, lax security measures may encourage leaks by causing employees to believe that classified information does not really require protection.

As a general rule, protective security programs serve a number of objectives besides prevention of unauthorized disclosures, and therefore this report does not consider these programs in great detail. The following observations are made:

-- Greater emphasis should be given to security education programs for senior officials.

-- Better controls on copying and circulation of classified documents would reduce dissemination and aid the task of investigating leaks.

-- The federal personnel security program under E.O. 10450 and implementing regulations should be revised and updated.

We also considered whether there should be a government-wide program to regulate contacts with media representatives by government officials with access to classified information. Such contacts, especially when they occur on a frequent and informal basis, may give rise to deliberate as well as negligent disclosures of classified information. However, the operational considerations among the agencies vary greatly. Therefore, each agency should be required to develop its own policy regarding contacts between journalists and employees who have access to classified information.

Past Experiences with Leak Investigations

Leaks are extremely difficult to investigate because they involve a consensual transaction. Both the leaking official and the receiving journalist have a strong incentive to conceal the source of the information.

Leak investigations do not focus on the receiving journalist for a variety of reasons. Rarely is there sufficient probable cause to justify a search or electronic surveillance of the

journalist. The use of some kinds of investigative techniques may raise First Amendment concerns to which we should be sensitive. Finally, journalists are unlikely to divulge their sources in response to a subpoena for documents or testimony before a grand jury, and contempt sanctions against journalists in other types of cases have not been effective.

Therefore, leak investigations generally focus on government employees who have had access to the information that is leaked. In most situations, hundreds or thousands of employees have had access to the information, and there is no practical way to narrow the focus of the inquiry. Also, the leaking official is unlikely to confess his offense in response to a simple inquiry. The polygraph can be an effective tool in eliciting confessions, but existing regulations do not permit compulsory use of the polygraph for many employees.

Leaks of classified information constitute a potential violation of the espionage laws and other statutes that fall within the FBI's investigative jurisdiction. (By contrast, many agencies that originate classified information are not authorized to go beyond their own employees in investigating leaks.) However, FBI has been reluctant to devote its resources to leak investigations. The burden of such investigations falls almost entirely on the Washington Field Office. Such investigations frequently involve high ranking government officials, who may be uncooperative. Sometimes a time-consuming investigation is undertaken, only to reveal that the source of the leak was a White House or Cabinet official who was authorized to disclose the information. Finally, it is very rare for an investigation to identify the leaking official, and even rarer that a prosecutable case is developed or that administrative action is taken against a leaker.

The Criminal Division of the Justice Department has developed the practice of screening leak cases before referral to FBI, for the purpose of eliminating those that are unlikely to lead to criminal prosecution. This practice involves the frequently criticized "eleven questions" that agencies are expected to answer when they report leaks to the Criminal Division and that include an advance commitment to provide and declassify such classified information as may be required to support a prosecution.

In summary, the past approach to leak investigations has been almost totally unsuccessful and frustrating to all concerned. There have been frequent disputes between the Justice Department and agencies complaining about leaks. This ineffectual system has led to the belief that nothing can be done to stop leaks of classified information.

Proposed New Approach to Leak Investigations

Unless new criminal legislation is enacted, we should recognize that leak investigations are unlikely to lead to successful criminal prosecutions. However, the present system would be greatly improved if employees who leak classified information could be identified and fired from their jobs. Therefore, we should recognize that the likely result of a successful leak investigation will be the imposition of administrative sanctions except for cases in which exacerbating factors suggest that criminal prosecution should be considered.

We should also recognize that resources are available to investigate only a small fraction of leaks. All leaks should be evaluated in light of criteria developed through consultation between the Justice Department and affected agencies. These criteria would include:

--the level of classified information disclosed;

--the resulting damage to national security;

--the extent to which the information had been disseminated at the time it was leaked; and

--the presence of specific "leads" to narrow the focus of investigation.

Agencies should be encouraged to conduct more extensive preliminary investigations before referring leaks to the Department of Justice for investigation. Affected agencies should be consulted by the Department of Justice in determining which leak cases warrant investigative priority. A decision to undertake criminal prosecution would not be required as a prerequisite to FBI investigation. FBI should be specifically authorized to investigate unauthorized disclosures that potentially violate federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

The polygraph is an investigative technique occasionally used in leak investigations. By regulation, most federal agencies are not permitted to take adverse actions against employees who refuse to be polygraphed. However, there is no constitutional or statutory bar to requiring federal employees to take a polygraph examination as part of an investigation of unauthorized disclosures of classified information. We recommend that existing

regulations be changed to permit greater use of the polygraph in leak investigations.

Use of the polygraph is a controversial technique, but security specialists believe it can be effective in situations where a leak investigation turns up a limited number of suspects. Under this approach the polygraph is used sparingly and as a last resort. Such polygraph examinations can be limited to the circumstances of the disclosure being investigated, and need not involve questions of a personal nature that some employees find offensive.

Finally, when investigations identify employees who have disclosed classified information without authority, they should not be let off with a slap on the wrist. The full range of administrative sanctions--including discharge--is available. Most employees have certain procedural rights, including notice, hearing and administrative appeal. However, an agency head who follows proper procedures should have no difficulty in disciplining or discharging leakers. It would be helpful for the Merit Systems Protection Board and other administrative bodies to adopt "graymail"-type procedures to protect classified information that may be involved in such situations.

Summary of Recommendations

1. The Administration should support new legislation to strengthen existing criminal statutes that prohibit the unauthorized disclosure of classified information.

2. All persons with authorized access to classified information should be required to sign secrecy agreements in a form enforceable in civil actions brought by the United States. For persons with access to the most sensitive kinds of classified information, these agreements should also include provisions for prepublication review.

3. Agencies should adopt appropriate policies to govern contacts between media representatives and government officials, so as to reduce the opportunity for negligent or deliberate disclosures of classified information.

4. Each agency that originates or stores classified information should adopt internal procedures to ensure that unauthorized disclosures of classified information are effectively investigated and appropriate sanctions imposed for violations.

5. The Department of Justice, in consultation with affected agencies, should continue to determine whether FBI investigation of an unauthorized disclosure is warranted. The FBI should be permitted to investigate unauthorized disclosure of classified information under circumstances where the likely result of a successful investigation will be imposition of administrative sanctions rather than criminal prosecution.

6. Existing agency regulations should be modified to permit the use of polygraph examinations for government employees under carefully defined circumstances.

7. All agencies should be encouraged to place greater emphasis on protective security programs. Authorities for the federal personnel security program should be revised and updated.